

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

U.S. DISTRICT COURT
DISTRICT OF N.H.
FILED

UNITED STATES OF AMERICA)
)
 v.)
)
 HIEU MINH NGO)

2014 MAR -5 A 10:36
1:12-cr-00144-PB

INFORMATION

The United States Attorney charges:

Introduction

At all times material to this Information:

1. Defendant HIEU MINH NGO ("NGO"), also known by online monikers that include "hieupc," "traztaz659," [REDACTED] and "Wan Bai," resided in Vietnam. He is the control person and administrator for websites including "findget.me" and "superget.info," and their associated data.
2. Personally identifiable information ("PII") can include individuals' names, addresses, social security numbers, dates of birth, places of work, duration of work, state driver's license numbers, mothers' maiden names, bank account numbers, bank routing numbers, e-mail account names, and other account passwords.
3. "Payment card data" refers to credit, debit, and/or gift card numbers and associated data that can be used to make charges on an account. The data typically includes the payment card number, expiration date, Card Verification Value ("CVV") number, account holder name, account holder address, and phone number.

4. "Carding" refers to an assortment of illegal activities revolving around the theft and fraudulent use of PII and payment card data, and "carders" refers to individuals who are engaged in illegal carding activity.
5. "Carder forums" are websites that provide an online marketplace for various carding activities. Typically, membership is required. Members can purchase a variety of types of goods and services, including other individuals' PII and payment card data. The members typically communicate via email messages, private messages, or via posts to the forum.
6. "Fulls" or "fullz" ("Full Info(s)") are slang terms that carders use to describe a package of PII. The defendant acquired and offered for sale "fullz" that typically included the following types of PII: names, addresses, social security numbers, dates of birth, places of work, duration of work, state driver's license numbers, mothers' maiden names, bank account numbers, bank routing numbers, e-mail account names, and other account passwords.
7. "Fullz" are frequently used by carders to take over the identity of a person in order to engage in various types of fraudulent activities, without the identity theft victim's consent. These can include opening new financial accounts in the victim's name and making fraudulent purchases on, or transfers of funds from, those accounts; taking out loans in the victim's name; and the filing of fraudulent tax refund requests with the Internal Revenue Service (IRS) on behalf of the victim.
8. "Liberty Reserve" ("LR") was an anonymous, offshore, electronic currency system that enabled individuals with LR accounts to transfer money through offshore accounts to other LR account holders worldwide. Transactions could be made anonymously, and the only form of identification that LR required to create an account was an e-mail address.
9. From 2007 through February 2013, the defendant acquired, offered for sale, sold, and/or transferred to others "fullz" of more than 150,000 individuals. He repeatedly acquired and transferred to others "fullz" of individuals including individuals located in the District of

New Hampshire. The bank account information contained in those “fullz” included bank branches located in the District of New Hampshire. Furthermore, he repeatedly sold and transferred “fullz” to one or more buyers located in the District of New Hampshire.

10. From 2007 through February 2013, the defendant acquired, offered for sale, sold, and/or transferred to others, stolen payment card data. The stolen payment card data typically included the victim account holder’s payment card number, expiration date, CVV number, account holder name, account holder address, and phone number. He repeatedly acquired and transferred to others stolen payment card data for account holders located in the District of New Hampshire.
11. From 2007 through February 2013, the defendant, while in Vietnam, administered websites, including “findget.me” and “superget.info,” to which he allowed more than one thousand (1,000) individuals from numerous countries, including the United States, to access databases that contained PII of hundreds of millions of United States citizens. The defendant allowed users of his website to conduct “queries,” where the user would input a particular first name and last name, and the defendant would then provide the user with the queried person’s associated PII, including the person’s date of birth and social security number. The defendant allowed his clients to conduct more than three million (3,000,000) such queries. Such queries included queries of individuals located in the District of New Hampshire.
12. The defendant was aware that the customers to whom he transferred fullz, payment card data, and the queried PII intended to use, and in fact often did use, that information to engage in criminal conduct, including to commit wire fraud, bank fraud, identity fraud, access device fraud, Automatic Teller Machine (ATM) fraud, and tax fraud.

COUNT ONE

**Wire Fraud
(18 U.S.C. §§ 1343 and 2)**

13. The allegations set forth in paragraphs 1 through 12 of the Information are re-alleged and incorporated as set forth herein.

14. Beginning at a date uncertain, but at least as early as 2007, the exact date being unknown to the government, and continuing to a date uncertain, but at least as late as February 2013, in the District of New Hampshire and elsewhere, the defendant,

HIEU MINH NGO,

devised and intended to devise, and aided and abetted others in devising, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises.

15. In furtherance of, and for the purpose of executing, such scheme and artifice to defraud, in the District of New Hampshire and elsewhere, the defendant,

HIEU MINH NGO,

transmitted and caused to be transmitted by means of wire communication, as more particularly described below, in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, including, but not limited to those set forth below at paragraph 28.

The Scheme

16. It was part of the scheme that the defendant did acquire, offer for sale, sell, and transfer to others, “fullz,” including “fullz” of individuals residing in New Hampshire, which information was to be used to engage in various types of fraudulent carding activities, including but not limited to opening financial and payment card accounts in these

individuals' names and making fraudulent charges on, or transfers of funds from, those accounts.

17. It was further part of the scheme that the defendant did acquire, offer for sale, sell, and transfer to others, stolen payment card data, including payment card data of individuals residing in New Hampshire, which information was to be used to engage in various types of fraudulent carding activities, including but not limited to making fraudulent charges on, or transfers of funds from, those accounts.
18. It was further part of the scheme that the defendant did allow others to purchase and obtain PII of millions of United States citizens. He allowed his customers to submit a "query" of a particular name in order to obtain that person's associated PII, including the person's date of birth and social security number. The defendant then obtained this PII from databases that were located in the United States and that had been established for lawful purposes. These databases contained PII of hundreds of millions of United States citizens, including individuals located in New Hampshire. The queried names included individuals located in the District of New Hampshire.
19. It was further part of the scheme that the defendant acquired payment card data of individuals, including individuals located in the District of New Hampshire.
20. It was further part of the scheme that the defendant acquired "fullz" of over 150,000 individuals, including individuals located in the District of New Hampshire.
21. It was further part of the scheme that the defendant operated one or more carder forums, including "superget.info" and "findget.me," where he stored and offered for sale "fullz" and other PII, including "fullz" of individuals located in the District of New Hampshire.
22. On the "superget.info" and "findget.me" carder forums, the defendant offered buyers the option either to obtain a specified quantity of "fullz" or to submit a "query" of a particular name in order to obtain that person's associated PII, including the person's date of birth and

social security number. As to the “fullz,” the defendant offered several categories of PII, depending on how “fresh” the data was (i.e., how recently the data had been acquired). The defendant typically charged higher prices for “fullz” that were “fresher” or acquired more recently.

23. It was further part of the scheme that the defendant had arrangements with “re-sellers,” including re-sellers who used the online monikers “attackervietnam” and “ssndob.sll.” The defendant charged a fee to these re-sellers, and in exchange, the re-seller could access and re-sell the defendant’s stolen payment card data, “fullz,” and other PII.
24. It was further part of the scheme that the defendant created one or more accounts with “Liberty Reserve” (“LR”) and used those accounts to receive funds for the stolen payment card data, “fullz,” queries made of databases, and other PII that he sold. The defendant instructed purchasers to create their own LR accounts in order to pay for the stolen payment card data, “fullz,” queries, and other PII. The defendant provided his LR account information to purchasers and instructed purchasers to transfer the required funds from the purchasers’ LR accounts into the defendant’s LR accounts.
25. It was further part of the scheme that the defendant opened various e-mail accounts, including “hieupc@gmail.com,” “traztaz659@gmail.com,” and [REDACTED]@gmail.com,” (all of which were maintained on servers in the United States but not in New Hampshire) and used those accounts to communicate with prospective and actual buyers and sellers, and to transfer stolen payment card data, “fullz,” and other PII.
26. It was further part of the scheme that the defendant, typically using those e-mail accounts, electronically transferred stolen payment card data, including payment card data belonging to individuals located in New Hampshire, to others.
27. It was further part of the scheme that the defendant, typically using those e-mail accounts, electronically transferred stolen “fullz,” including “fullz” of individuals located in New

Hampshire, to other buyers, including to one or more buyers located in the District of New Hampshire.

Wire communications in Interstate and Foreign Commerce

28. In furtherance of, and for the purpose of executing the scheme, the defendant transmitted, and caused to be transmitted, several wire communications in interstate and foreign commerce, including the following:

- A. On or about November 21, 2011, NGO sent an e-mail from Vietnam to a person he believed to be a customer but who was an undercover United States Secret Service Agent (US Agent) in the District of New Hampshire, regarding the username and password for the findget.me website.
- B. On or about November 29, 2011, NGO sent an e-mail from Vietnam to the UC agent, in the District of New Hampshire, containing 245 “fullz” including for New Hampshire residents;
- C. On or about December 5, 2011, NGO sent an e-mail from Vietnam to the UC agent, in the District of New Hampshire, containing 90 “fullz” including for New Hampshire residents.

Acts in Furtherance of the Scheme

29. In furtherance of the scheme, and to effect and accomplish it, the defendant committed, among others, the following acts in the District of New Hampshire and elsewhere:

Setting Up Carding Web Sites, E-mail Accounts, and Liberty Reserve Accounts

- 30. On or about July 3, 2010, NGO registered the domain name “superget.info” with Domains by Proxy LLC, a webhosting company and registrar with computer servers located in Arizona.
- 31. On or about December 14, 2010, NGO subscribed for a webhosting account with VPS.net and obtained “cloud hosting” services from VPS.net for purposes of storing large amounts of

electronic data. NGO continued to pay the monthly fee at least through October 2012.

VPS.net is a webhosting company based in Utah with computer servers located in Illinois.

32. On or about November 18, 2011, NGO registered the domain name "findget.me" with

Domains by Proxy LLC, located in Arizona.

33. On or about May 18, 2010, NGO created an e-mail account with Google for the account

name [REDACTED]@gmail.com." In the account subscriber records, NGO identified [REDACTED]
[REDACTED] as the subscriber.

34. On or about March 10, 2009, NGO created an e-mail account with Google, for the account

name [REDACTED]@gmail.com."

35. In or before January 2010, NGO opened a Liberty Reserve account for use in buying and

selling payment card data, "fullz," and other PII.

36. In or before November 2011, NGO opened a Liberty Reserve account, using the name [REDACTED]

[REDACTED] (which NGO had identified as the subscriber in opening the trazitaz659 Gmail account) for use in buying and selling payment card data, "fullz," and other PII.

Storing Stolen PII

37. On or before December 2011, NGO stored "fullz" for over 150,000 individuals on the

"findget.me" website. These included "fullz" of one or more individuals located in the District of New Hampshire.

Transferring New Hampshire Residents' "Fullz" and Stolen Payment Card Data

38. On or about November 29, 2007, NGO, using the e-mail account "hieupc@gmail.com," sent

an email message to [REDACTED]@gmail.com" that contained stolen payment card data for approximately 300 individuals (including payment card numbers, expiration date, CVV number, account holder names, account holder address), as well as what appears to be the

account holder's Internet Protocol ("IP") address, at least three of whom are New Hampshire residents.

39. On or about November 30, 2007, NGO, using the "hieupc" e-mail account, sent an email message to "[REDACTED]@gmail.com" that contained stolen payment card data for approximately 200 individuals (including payment card numbers, expiration date, CVV number, account holder names, account holder address), as well as what appears to be the IP address, at least two of whom are New Hampshire residents.
40. On or about December 8, 2007, NGO, using the "hieupc" e-mail account, sent an email message to "[REDACTED]@gmail.com" that contained stolen payment card data for approximately 300 individuals, as well as what appears to be the account holder's IP address, at least four of whom are New Hampshire residents.
41. On or about October 2, 2009, NGO, using the "hieupc" e-mail account sent an email message to "[REDACTED]@yahoo.com" that contained stolen payment card data for approximately 117 individuals, as well as what appears to be the account holder's mailing address, email address, at least one of whom is a New Hampshire resident.
42. On or about January 15, 2010, NGO, using the "hieupc" e-mail account, sent an email message to "[REDACTED]@gmail.com" that contained stolen payment card data for approximately 72 individuals, as well as what appears to be the account holder's mailing address and phone number, at least one of whom is a New Hampshire resident.
43. On or about June 2, 2011, NGO, using the "hieupc" e-mail account, sent an e-mail message to "[REDACTED]@gmail.com" that contained "fullz" of approximately 660 New Hampshire residents.
44. On or about September 21, 2011, NGO, using the e-mail account "traztaz659@gmail.com," sent an e-mail to "[REDACTED]@yahoo.com" that contained "fullz" for approximately 31 people, including at least one New Hampshire resident.

45. On or about September 26, 2011, NGO, using the "traztaz659" e-mail account, sent an e-mail to [REDACTED]@gmail.com" that contained "fullz" for approximately 2,160 people, including at least nine New Hampshire residents.
46. On or about September 29, 2011, NGO, using the "traztaz659" e-mail account, sent an e-mail to [REDACTED]@gmail.com" that contained "fullz" for approximately 2,600 people, including at least five New Hampshire residents.
47. On or about November 18, 2011, NGO, using the e-mail account [REDACTED], sent an e-mail to [REDACTED]@gmail.com" stating, "Hi mate! It's still normal for everything. \$4600 for 4000 credits and \$500 for server fee. Please pay to our LR: U8109093 [REDACTED] Thanks u."
48. On November 19, 2011, NGO, using the e-mail account "rr2518," forwarded to NGO, at "hieupc@gmail.com," an email from [REDACTED]@gmail.com," which appeared to be written in Vietnamese, and asked, "I don't know what he wrote, can you help me?" NGO later sent an e-mail directly to "ssndob.sll," explained that the person who sent the e-mail (in an apparent attempt to hide his involvement) does not understand Vietnamese, and offered to translate into English.
49. On November 26, 2011, Ngo, using the e-mail account [REDACTED]" sent an email to 13 email addresses with the subject line "hi guy [admin of findget.me]," stating, "Hi, I see you as a big customer at findget.me. If you want to have a big deal with us, please let us know. Currently we have some big plans for users like you" \$5000 for 22,000 credits. \$10,000 for 50,000 credits. (with fully 24/24 hours support from admin if you have any issues. Thank you."
50. On December 2, 2011, NGO, using the "traztaz659" e-mail account, sent an e-mail to [REDACTED]@gmail.com" that contained "fullz" for approximately 270 people.
51. On December 15, 2011, NGO, using the e-mail account [REDACTED] sent an e-mail to [REDACTED]@yahoo.com" that contained "fullz" of approximately 420 individuals.

52. On December 23, 2011, NGO, using the e-mail account "[REDACTED]" sent an email to [REDACTED] that contained "fullz" of approximately 200 individuals.
53. On December 27, 2011, NGO, using the e-mail account [REDACTED] sent an email to [REDACTED] that contained "fullz" of approximately 105 individuals.
54. On December 19, 2011, NGO, using the e-mail account [REDACTED]' sent an email to [REDACTED]08@gmail.com" that contained "fullz" of approximately 520 individuals.
55. On January 9, 2012, NGO, using the e-mail account [REDACTED] sent an email to [REDACTED]@yahoo.com" that contained "fullz" of approximately 220 individuals.
56. On the same date, NGO, using the e-mail account [REDACTED] sent an email to [REDACTED]@yahoo.com" that contained "fullz" of approximately 20 individuals' PII.
57. On January 10, 2012, NGO, using the e-mail account [REDACTED] sent an email to [REDACTED] gmail.com" that contained "fullz" of approximately 270 individuals.
58. On January 24, 2012, NGO, using the e-mail account [REDACTED] sent an email to [REDACTED]@yahoo.co.uk" that contained "fullz" of approximately 22 individuals.

Offering to Sell Stolen PII to Undercover Agent in New Hampshire

59. In or about November 2011, a member on the carder forum "findget.me" instructed a visitor to that forum to send an e-mail message to [REDACTED]@gmail.com" in order to open an account with "findget.me." Unbeknownst to the defendant, the visitor was an undercover agent located in New Hampshire ("UC agent"). He also instructed that UC agent to open an account with "Liberty Reserve" in order to engage in any financial transactions with them.
60. On or about November 21, 2011, NGO sent an e-mail message to the UC agent with a username and password for him to use in order to open an account with findget.me, and created an account on "findget.me" on behalf of the UC agent.

61. From in or about November 29, 2011, through in or about February 2013, NGO, using the e-mail account [REDACTED] engaged in a series of e-mail communications with the UC agent in which he discussed the UC agent's interest in purchasing "fullz."

Transferring "Fullz" to Undercover Agent in New Hampshire

62. On or about November 29, 2011, after the UC agent purchased "fullz" from [REDACTED] using Liberty Reserve, NGO sent an e-mail message to the UC agent that contained "fullz" of approximately 245 individuals and included New Hampshire residents.

63. Also on or about November 29, 2011, after the UC agent purchased "fullz" from [REDACTED] using Liberty Reserve, NGO sent an e-mail message to the UC agent that contained "fullz" of approximately 50 individuals, including New Hampshire residents.

64. On or about December 5, 2011, after the UC agent purchased "fullz" from [REDACTED] using Liberty Reserve, NGO sent an e-mail message to the UC agent that contained "fullz" of approximately 90 individuals and included New Hampshire residents.

65. On or about June 5, 2012, after the UC agent sent an e-mail message to NGO stating that he wanted to "buy some really fresh fullz for New Hampshire males between 18-40 years. The ones I bought before I couldn't open credit cards and almost got caught. J how much for 25? How fresh are they?," NGO sent an e-mail message back to the UC agent that responded ".5\$ per one info".

In violation of Title 18, United States Code, Sections 1343 and 2.

COUNT TWO

**Identification Fraud
(18 U.S.C. §§ 1028(a)(7) & 2)**

66. The allegations set forth in paragraphs 1 through 12, 15 through 64 of the Information are re-alleged and incorporated as set forth herein.

67. Beginning on or about the dates set forth below, the exact date being unknown to the government, and continuing to February 2013, in the District of New Hampshire and elsewhere, as set forth below, the defendant

HIEU MINH NGO

knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, namely, “fullz” of individuals residing in the District of New Hampshire and elsewhere, with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law and that constitutes a felony under any applicable State and local law, including: a) access device fraud, in violation of 18 U.S.C. § 1029(a)(2); b) aggravated identity theft, in violation of 18 U.S.C. § 1028A; and, c) wire fraud, in violation of 18 U.S.C. § 1343. The defendant specifically transferred, possessed, and used, without lawful authority the following means of identification, as well as others, on the following dates:

Information Transferred	Date of Transfer
“Fullz” containing 660 New Hampshire residents’ fullz	6/2/11 NGO e-mail to [REDACTED]@gmail.com”
“Fullz” containing 9 New Hampshire residents’ fullz	9/29/11 NGO e-mail to [REDACTED]@gmail.com”
“Fullz” of 245, including for New Hampshire residents	11/29/11 NGO e-mail to New Hampshire UC agent
“Fullz” of 90, including for New Hampshire residents	12/5/11 NGO e-mail to New Hampshire UC agent

In violation of Title 18 United States Code, Sections 1028(a)(7) and 2.

COUNT THREE

**Fraud in Connection with Access Devices
(18 U.S.C. §§ 1029(a)(2) & 2)**

68. The allegations set forth in paragraphs 1 through 12, 15 through 64 of the Information are re-alleged and incorporated as set forth herein.

69. Beginning on or about the dates set forth below, the exact date being unknown to the government, and continuing to February 2013, in the District of New Hampshire and elsewhere, as set forth below, the defendant

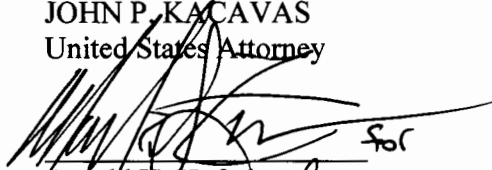
HIEU MINH NGO

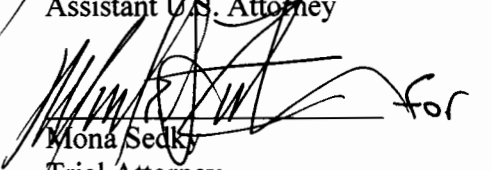
knowingly and with intent to defraud trafficked in and used one or more unauthorized access devices, specifically including, but not limited to, “fullz” and payment card data of individuals residing in the District New Hampshire and elsewhere, during a one-year period and by such conduct obtained anything of value aggregating \$1,000 or more during that period, said conduct affecting interstate and foreign commerce.

In violation of Title 18, United States Code, Sections 1029(a)(2) and 2.

March 5, 2014

JOHN P. KACAVAS
United States Attorney

 for
Arnold H. Huftalen
Assistant U.S. Attorney

 for
Mona Sedky
Trial Attorney
U.S. Department of Justice